National Infrastructure Protection Center
CyberNotes

Issue #26-99 *December 22, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

The editor and writers of CyberNotes would like to wish everyone a safe and Happy New Year. CyberNotes will not be published on the 5 of January but will start again on the 19th.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 4, and December 17, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Alpha Linux[1]	Alpha Linux	Several buffer overflow vulnerabilities exist which will allow a malicious user to run arbitrary commands.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Securiteam, December 7, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Apple[2] ***Exploit has appeared in the Press.***[3]	**MacOS 9.0**	**The NDS client for MacOS 9 fails to log the user out of the NDS tree when he/she logs out of the MacOS 9 system. The next user to log in to the machine will inherit the previous user's NDS access.**	**No workaround or patch available at time of publishing. Unofficial workaround: Always log out of NDS first.**	**NDS Client Inherited Login Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Cisco[4]	Cache Engine 2050, Release 1.0 through 1.7.6; Cache Engine 550, Release 2.0.1 through 2.0.2	Vulnerability exists which could allow a malicious user to substitute arbitrary material in place of legitimate content for a specified website. A second vulnerability exists which could allow a malicious user to view performance information via the web interface of the Cache Engine. A third vulnerability exists which allows a null username and password pair to be accepted as valid authentication credentials.	Patch is located in the Software Center under the title "Cisco Web Cache Engine" located at: http://www.cisco.com	Cache Engine Authentication Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Debian[5]	Debian GNU/Linux 2.1 Sendmail	A malicious user who attempts to regenerate the aliases databases and then interrupts it, can corrupt the database.	Recommend that you upgrade your Sendmail package to a new version located at: http://security.debian.org/dists/stable/updates/source/sendmail_8.9.3-3slink1.diff.gz	Database Regeneration Vulnerability	Medium	Bug discussed in newsgroups and websites.
FTP Servers[6]	FTP Servers	It is possible to cause certain types of FTP servers to stop responding by issuing multiple PORT commands in one session.	No workaround or patch available at time of publishing.	PORT Command Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
GoodTech Systems, Inc.[7]	GoodTech Telnet Server NT v2.2.1	A remote Denial of Service vulnerability exists when a long user name of 23870 characters is used.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[2] SecurityFocus, November 14, 1999.

[3] MSNBC, December 16, 1999.

[4] Cisco Advisory, December 16, 1999.

[5] Debian Security Advisory, December 7, 1999.

[6] Bugtraq, December 7, 1999.

[7] UssrLabs, December 6, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[8]	HP9000 series 7/800 servers running HP-UX release 11.00	Multiple vulnerabilities in the wu-ftp software exist which allow any user to gain root privileges.	Install patch PHNE_18377	Multiple Wu-Ftp Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Infoseek[9]	Ultraseek 2.1 to 3.1 (NT version only)	A Denial of Service vulnerability exists in the HTTP Get command.	Patch available at: http://software.infoseek.com/products/ultraseek/upgradt_nt.htm	Remote Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[10]	Linux 2.0.36, 2.0.38	A local Denial of Service vulnerability exists when the command: "ping –s 65468 –R some_IP_address" is run.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Mechfire[11]	War FTP Daemon 1.70 beta 1 sub-release 4, 1.70, 1.66	A vulnerability exists which makes it possible to cause the WarFTP Daemon to crash and possibly execute arbitrary code by opening multiple simultaneous connection.	No workaround or patch not available at time of publishing.	Denial of Service Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

Microsoft[12]	Windows NT Workstation 4.0;
	Server 4.0;
	Server 4.0 Enterprise Edition;
	Serrver 4.0 Terminal Server Edition
		Vulnerability exists which allows a particular cyptanalytic attack to be effective against Syskey, significantly reducing the strength of the protection it offers.	A patch can be found at:
			http://www.microsoft.com/Downloads/Release.asp?ReleaseID-16798
				Syskey Keystream Reuse Vulnerability	Medium	Bug discussed in newsgroups and websites.
						Exploit has been published.

Microsoft[13]	Internet Explorer 5.0	A buffer overflow condition exists when Internet Explorer evaluates a URL that contains "nd.ms.radip:\\aaaaaaa…", this could allow a malicious user to execute arbitrary code.	This may have been fixed already in a recent patch. The following versions have been reported to be non-vulnerable:
			5.00.2014.0216;
			5.50.3825.1300;
			5.00.2920.0000
				Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites.
						Exploit has been published.

[8] Hewlett-Packard Security Advisory, HPSBUX9912-106, December 13, 1999.
[9] UssrLabs and eEye Digital Security Team, December 15, 1999.
[10] Securiteam, December 14, 1999.
[11] UssrLabs, December 14, 1999.
[12] Microsoft Security Bulletin, MS99-056), December 16,1 999.
[13] Bugtraq, December 5, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[14]	MS SQL Server 7.0	It is possible to change the password of SA on an MS SQL Server without using any of the administrative tools provided with MS SQL Server. This allows gaining of higher privileges on the server.	Microsoft acknowledges that the vulnerability scenario works but it relies on several critical mistakes having already been made by the system administrator. They suggest reading the SQL Server Security reference located at: http://www.microsoft.com/sql/DeployAdmin/Security.doc	SQL Password Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published. This vulnerability has appeared in the press.

Microsoft[15]	Windows NT Workstation 4.0;
	Server 4.0;
	Server 4.0 Enterprise Edition;
	Serrver 4.0 Terminal Server Edition
		Vulnerability exists which could allow a malicious user to cause a Windows NT machine to stop responding to requests for service.	The fix for this vulnerability is included in the patch for the “Syskey Keystream Reuse” vulnerability which can be found at:
			http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16798
				Malformed Security Identifier Request Vulnerability	Low	Bug discussed in newsgroups and websites.

Netscape[16]	Enterprise Server for NetWare 4/5 3.0.7a	The Admin feature is vulnerable to a Denial of Service attack due to a buffer overflow in admserv.nim during the login procedure.	No workaround or patch available at time of publishing. Unofficial workaround: The Admin Server port can be blocked at the firewall, to prevent attacks from remote networks.	Admin Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites.
OpenBSD[17]	OpenSSH-1.2.0 and earlier; SSH 1.2.27	A malicious ssh-client can force a server to use the cipher “none” even if the server-policy does not permit this.	A patch for the versions of OpenSSH shipped with OpenBSD-2.6 is available at: http://www.openbsd.org/errata.html#sshjumbo	Unencrypted Session Vulnerability	Medium	Bug discussed in newsgroups and websites.
RedHat[18]	RedHat Linux 6.1, Intel and SPARC	ORBit and gnome-session each contain a Denial of Service Vulnerability. ORBit and esound contain a security hole, which allows a malicious user, with local access, to guess the authentication keys used to control access to these services.	Patch available at: ftp://updates.redhat.com/6.1/i386/ORBit-0.5.0-2.i386.rpm ftp://updates.redhat.com/6.1/i386/esound-0.2.17-1.i386.rpm ftp://updates.redhat.com/6.1/i386/gnome-core-1.0.54-2.i386.rpm	Denial of Service and Security Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
SCO[19]	Unixware 7.0, 7.0.1, 7.1, 7.1.1	Vulnerability in Unixware’s implementation of privileges allows regular users to attach a debugger to a running privileged program and take over its privileges.	No workaround or patch available at time of publishing.	Privileged Program Debugging Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[14] Securiteam, December 13, 1999.
[15] Microsoft Security Bulletin, MS99-057, December 16, 1999.
[16] SecurityFocus, December 9, 1999.
[17] Bugtraq, December 14, 1999.
[18] RedHat Security Advisory, RHSA-1999:058-01, December 12, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SCO[20]	Unixware 7.1	By exploiting a buffer overflow in pkgcat and pkginstall, it is possible to view the entries in /etc/shadow.	No workaround or patch available at time of publishing. Unofficial workaround is to remove the entries from /etc/security/tcb/privs.	Buffer Overflow Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
SCO[21]	Unixware 7.1	Any user can read/modify others' mail due to misconfigured permission settings on the /var/mail directory.	No workaround or patch available at time of publishing.	E-mail Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Stalker Software[22]	CommuniGatePro 3.1 for Windows NT	A remote Denial of Service vulnerability exists.	This has been fixed in the current 3.2 beta version. Please install either the 3.2b5 or the 3.2b7 version located at: http://www.stalker.com/CommuniGatePro	Remote Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[23]	Solaris 2.5, 2.5_x86, 2.5.1, 2.5.1_ppc, 2.5.1_x86, 2.6, 2.6_x86, 2.7, 2.7_x86	All versions of sadmind are vulnerable to a buffer overflow that can overwrite the stack pointer within a running sadmind process. Since sadmind is installed as root, it is possible to execute arbitrary code with root privileges on a remote machine.	Sun Microsystems is currently working on patches to address this issue and recommends disabling sadmind until a patch is released.	Sadmind Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Microsystems[24]	Solaris 2.6, 2.7, 5.5.1, 5.6	A malicious user can read files, which they wouldn't have read access to, allowing them to gain additional information about the system (passwords, hosts, configuration, etc.	No workaround or patch available at time of publishing.	Security Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[25]	SunOS 5.7, 5.7_x86, 5.6, 5.6_x86, 5.5.1, 5.5.1_X86, 5.5_X86, 5.4, 5.4_X86, 5.3	Snoop captures packets from the network and displays their contents. Buffer overflow vulnerability exists in this application and a remote malicious user can execute arbitrary instructions and gain root.	Patch available at: http://sunsolve.sun/com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches	Snoop Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[19] SecurityFocus, December 10, 1999,

[20] SecurityFocus, December 6, 1999.

[21] Securiteam, December 6, 1999.

[22] NTBugtraq, December 3, 1999.

[23] CERT Advisory, CA-99-16, December 14, 1999.

[24] Securiteam, December 4, 1999.

[25] Bugtraq, December 6, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Various Systems[26]	Systems running some versions of sshd; systems using products that use RSAREF2 Library	Some versions of sshd are vulnerable to a buffer overflow that can allow a malicious user to influence certain variables internal to the program. This vulnerability alone does not allow a malicious user to execute code. However, a vulnerability in RSAREF2 can be used in conjunction with the vulnerability in sshd to allow a remote intruder to execute arbitrary code.	Apply patch(es) from your product vendor.	SSH Daemon and RSAREF2 Library Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
VDO[27]	Live Player 3.0	VDO Live Player contains a buffer overflow that is cause by a '.vdo' file that contains a long vdo address. If the VDO Live Player is installed on the system and the default setting of the browser are used, '.vdo' files are downloaded and executed without any confirmation.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

Whois[28]	Whois Internic Loopup version 1.0;
	CC Whois version 1.0;
	Matt's Whois Version 1
		Due to the lack of shell escape character parsing, Whois CGI allows the execution of arbitrary commands.	No workaround or patch available at time of publishing.	Security Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[26] CERT Advisory, CA-99-15, December 13, 1999.
[27] Securiteam, December 14, 1999.
[28] Whois.CGI Advisory, hhp-ADV#12, December 12, 1999.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between December 3, and December 16, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 72 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**	**Comments**
December 16, 1999	Hhopen.txt	Exploit script for the HHOPEN.OCS vulnerability in IE5 that allows the execution of arbitrary code.	
December 16, 1999	Trash2.c	Denial of Service attack against Windows 98/95/2000/NT machines.	
December 16, 1999	Ultraseek.remote.txt	Infoseek Ultraseek 3.1 for NT exploitable remote buffer overflow vulnerability script.	
December 16, 1999	Netfilter-0.1.13.tar.bz2	A framework for arbitrary packet mangling.	
December 15, 1999	Ssh-1.2.27-exploit.txt	Exploit for SSH-1.2.27 compiled with RSAREF2 for Linux (RedHat 6.0) and OpenBSD 2.6.	
December 15, 1999	Xsoldier.c	Exploit script for the FreeBSD 3.3's xsoldier vulnerability, which allows any user to gain root access.	
December 15, 1999	Redir-2.2.tar.gz	A port redirector whose functionality consists of the ability to listen for TCP connections on a given port, and when it receives a connection, redirect that connect to a given destination address/port, and pass data between them.	
December 14, 1999	**Sadmindscan.c**	**Sadmind Solaris RPC tiny scanner that scans a specific host or a class C network.**	
December 14, 1999	Ttysnoop-0.12d.tar.gz	TTYSnoop allows you to snoop on login tty's through another tty-device or pseudo-tty.	
December 14, 1999	**Warftp.dos.txt**	**Technique to exploit the vulnerability in the War FTP Daemon 1.70.**	
December 13, 1999	**Sadmind.scan.c**	**Mass scanner for rpc.sadmind.**	
December 13, 1999	**Sadmind.txt**	**Exploit technique for the Solaris sadmind vulnerability.**	
December 13, 1999	**Sadmindex-brute-lux.c**	**Sadmind exploit stack pointer brute forcer.**	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
December 13, 1999	**Msadcscan-unix.c**	**A basic string scanner that scans for the msadc module string.**	
December 13, 1999	**MDAC-scan.c**	**Msadc scanner written in C.**	
December 13, 1999	**Whois.cgi.txt**	**Exploit technique for the whois cgi packages vulnerability.**	
December 13, 1999	Winfingerprint-22.zip	Advanced remote Windows OS detection.	
December 13, 1999	Cgichk-s.pl	Cgichk CGI scanner written in perl, modified to scan class C networks.	
December 13, 1999	Ircnet.topic.txt	Technique that can be used against the IRCnet’s IRCD vulnerability.	
December 13, 1999	Neped-libnet.tar.gz	Network Promiscuous Ethernet Detector, rewritten with Libnet/libpcap so it works on FreeBSD, OpenBSD, and Linux, which scans your subnet and detects promiscuous boxes that might be running sniffers or similar applications.	
December 13, 1999	Arp-ping.c	Attempts to identify boxes on your LAN run IP stack.	
December 13, 1999	**Nmap-2.3BETA10.tgz**	**A utility for port scanning large networks.**	
December 10, 1999	**Unixware7.fundamental.txt**	**Exploit technique for SCO UnixWare’s security vulnerability, which allows root access.**	
December 10, 1999	Veganizer-0.04.tar.gz	A spam counter-attack which searches the headers of a specified message for all associated IP’s and Domains, then sends mail to pre-specified addresses at those servers, as well as, addresses found by a whois query on the Ips/Domains.	
December 10, 1999	Punk.c	Syn Flooder source code with spoofed source address.	
December 10, 1999	Messala-1.5-BETA.tar.gz	Vulnerability scanner which scans for 97 CGI vulnerabilities, 7 FTP vulnerabilities, all known QPOP vulnerabilities, 7 named vulnerabilities and prints out which version the host is running on, 9 IMAP vulnerabilities, and 16 mail vulnerabilities.	
December 10, 1999	Suicide.sh	WindowMaker 0.60.0 Denial of Service exploit script.	
December 10, 1999	Autofdscan.c	RPC.AutoFS tiny scanner.	
December 9, 1999	Qpop-linux	Remote buffer overflow exploit in perl for QPOP3.0b<=20 running on Linux.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
December 9, 1999	Solaris.snoop.c	Exploit script for the snoop vulnerability.	
December 9, 1999	**Ex_vdolive.c**	**Remote exploit script for the VDO LivePlayer 3.02 vulnerability.**	
December 9, 1999	Blitznet.tgz	Launches a distributed syn flood attack with spoofed source IP, without logging.	
December 9, 1999	**Trinoo.tgz**	**Trinoo daemon source, which implements a distributed Denial of Service attack, controlled via UDP.**	**See write-up below.**
December 9, 1999	Nscache-0.2pl1.tgz	A simple program to browse the Netscape cache directory with a GTK UL.	
December 9, 1999	Frontpage.2000.txt	After upgrading to Front Page 2000 extensions, all Front Page webs are vulnerable to be opened, modified, or deleted by anyone without entering a password.	
December 9, 1999	Icqrinfo.zip	A Windows program that reads information (including password) out of ICQ.DAT (versions 99a and 99b).	
December 8, 1999	Rtscan.pl	Perl script which scans a remote system for about 150 Trojans.	
December 8, 1999	Getcode0.10.lzh	Assists you in coding Windows exploits by getting the codes for jmp reg.call, reg.push, regret from some loaded dlls.	
December 8, 1999	Ie.frameloop.txt	Exploit technique that can used against IE4 and IE5's Frame Loop Vulnerability.	
December 8, 1999	Portfwd-0.7.tar.gz	A small C++ utility that forward incoming TCP connections and/or UDP packets to remote hosts.	
December 7, 1999	Pro-lite.zip	A database for the OmniRemote Palm Pilot program, which allows you to reprogram Pro-Lite brands of LED, signs.	
December 7, 1999	Nmap-2.3BETA9.tgz	A utility for port scanning large networks.	
December 7, 1999	**Saint-1.4.1.beta1.tar.gz**	**A security assessment tool based on SATAN.**	
December 7, 1999	Krnsniff.c	A kernel based sniffer module tested on Linux 2.2.5 kernel.	
December 7, 1999	Logcalls.c	Kernel module, which logs specific system calls to a logfile.	
December 7, 1999	Idlescan-x0.1-alpha3.tgz	An IP ID port scanner.	
December 7, 1999	Ipidscan-0.1beta1.tar.gz	IP ID port scanner, which is totally untraceable.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
December 7, 1999	Ie5.vns.ms.radito.txt	IE5 remote exploit script for the “vnd.ms.radio:\\aaaaaaa…” vulnerability.	
December 7, 1999	**Ftpd.dos.pl**	**Denial of Service exploit for many FTP daemons.**	
December 7, 1999	Dumpvmem.c	Windows NT, SP4 and below, password plaintext vulnerability exploit script.	
December 7, 1999	Audpbackdoor.tar.gz	An UDP based backdoor, client and server are written in perl.	
December 6, 1999	Sportal-1.9.5.tar.gz	Monitors files that you select for “hot words” that you also select, through a graphical interface.	
December 6, 1999	Portfwd-0.4.tar.gz	A small C++ utility that forwards incoming TCP connections and/or UDP packets to remote hosts.	
December 6, 1999	Weakness.zip	A DOS/Window command-line utility that will scan a target host for 94 known CGI vulnerabilities.	
December 6, 1999	Exo-0.3.tgz	A tool that sweeps a range of ports on a list of hosts.	
December 6, 1999	**Wu25.c**	**Another wu-ftpd 2.5.0 exploit, which finds world writable directories automatically.**	
December 6, 1999	Phasma_full.zip	A GUI based anonymous e-mailer, which allows you to enter arbitrary mail headers.	
December 6, 1999	Cgiback.tgz	CGI backdoor that can be compiled with or without logging.	
December 6, 1999	**Goodtech.telnet.dos.txt**	**A remote Denial of Service exploit technique for the GoodTech Telnet Server buffer overflow vulnerability.**	
December 6, 1999	Nemesis-v0.7.tar.gz	The Nemesis Project is designed to be a commandline-based, portable human IP stack for Unix/Linux.	
December 6, 1999	Multi-DoS.pl	A perl script, which exploits recent Denial of Service overflows in about 14 different Windows-based servers.	
December 6, 1999	Rpc.autofsd-bsd.c	A remote root exploit script for BSD.	
December 6, 1999	Pak-DoS.pl	Perl script which exploits the remote Denial of Service vulnerabilities in PakMail v1.25.	
December 6, 1999	Pakmail.txt	Exploit scripts that for the PakMail V1.325 Denial of Service vulnerability.	
December 6, 1999	**Unixware.pkg.exploits.txt**	**Script for UnixWare’s pkg commands which can be exploited to print /etc/shadow, leading to a probable root compromise.**	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
December 6, 1999	Galt_gin.c	Modification of the gin attack which can make a remote modem run any command.	
December 6, 1999	Spsend.tar.gz	A UDP/TCP IP packet sender with syn flood, land attack and spoofing.	
December 6, 1999	Netscape.msredir.txt	Exploit technique for the Netscape HTML vulnerability.	
December 6, 1999	**Unixware7.mail.txt**	**Exploit technique, which can be used to trap all incoming mail.**	
December 6, 1999	Bindshell-unix	Remote Unix shell backdoor written in perl.	
December 3, 1999	Loockout-1.2.zip	A Windows tool that sends raw data over a TCP connection, allowing the inspection of protocols and the testing of buffers.	
December 3, 1999	Evdsb7re.zip	A program, which lets you, configure and remove a SubSeven server, including some of its hidden features.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wishes to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

TRINOO

The notion of distributed intruder attacks is not necessarily new, but has evolved to the point where even a novice hacker could do serious damage. In a typical distributed attack scheme, the intruder or *attacker* controls a small number of *masters*, which in turn control a large number of *daemons*. These daemons can be used to launch various forms of packet floods or other attacks against select *targets* (victims) by the attacker. Two such recent distributed denial-of-service (DoS) attacks are Trinoo (pronounced tree-new) and Tribe Flood Network. A brief overview of Trinoo is discussed below.

The architecture of the Trinoo can be broken down into four components; the attacker's client, the Trinoo master, the trinoo daemon, and the victim. An attack is initiated when the attacker can use any client computer to contact a trinoo master across the Internet (typically through a TELNET session). The attacker must authenticate to the trinoo master by entering the correct password. Once the attacker has successfully authenticated, she has several options: specify the number of seconds to run the flood attack, kill all active daemons, kill the master, and an option to launch UDP-based flood attacks on a single or multiple targets. Once the trinoo master is provided a victim to flood, it contacts all of its trinoo daemons to initiate a flood attack. The flood will continue for a time period that is specified by the attacker, and is limited by the trinoo daemons to no longer than 1000 seconds (approximately 16 minutes, but can be easily modified in the source code). The addresses of the trinoo master(s) is also hard-coded in the source-code of each trinoo daemon, which sends a *HELLO* message to the master when started. It is important to note that none of the network communications between attacker, master, and daemon are encrypted. Versions of Trinoo have been discovered on UNIX-based systems running Solaris 2.x and Linux.

Trends

Trends for this two-week period:

- **Co-ordinated distributed attack methods which uses two exploit applications to formulate this type of attack: trin00 and Tribe Flood Network (TFN).**
- There has been an increase in attacks using three different RPC services vulnerabilities.
- The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.
- New variations of the Melissa virus continue to appear.
- Numerous systems are being root compromised via one of the most recent vulnerabilities in BIND.
- An increase in UDP scans on port 31789.
- An increase in ICMP Echo Reply Probes where no corresponding echo replies.
- **Numerous sites are being compromised via vulnerabilities in IIS web servers and MS Data Access Components (MDAC) vulnerabilities. (CyberNotes 99-22).** The Microsoft Data Access Components (MDAC), a part of Windows NT, and the RDS (Remote Data Services) DataFactory object vulnerabilities are currently the primary means for successful attacks on NT systems.
- An increase in widespread probes to port 98/tcp has been seen.
- Two vulnerabilities are being used together to gain access to vulnerable systems. The first is rpc.statd, a program used to communicate state changes among NFS clients and servers. The second is in automountd, a program used to automatically mount certain types of file systems.
- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP ports 80, 8080 and 3128.
- Intruders are using distributed network sniffers to capture usernames and passwords. UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.
- Increased intruder activity has been noticed involving the am-utils package.
- An increase in widespread probes to port 21/tcp has been seen.

Viruses

W95.Babylonia: The virus is unique because it has the ability to download its viral components from the Internet. When the virus arrives on a PC user's system, it will wait until the user makes an Internet connection. When the virus detects that the computer has accessed the Internet, it connects with a Web server located in Japan. Because the virus has such capability, it is possible for the virus writer to update the virus - and its effects on infected PCs - daily, hourly, or every second. Because the virus is updateable, the results of being infected with the virus can also change.

The virus is very complex, propagating to other computer users mainly via MIRC, a text-based communications application used to chat over the Internet. When an infected user logs onto MIRC, it will automatically send the virus to everyone within the same MIRC chat room as the infected user.

The virus is currently be sent as a Y2K bug fix. Once this purported bug fix is executed, it will infect 32-bit EXE program files and also Windows Help files.

The virus will try to modify an infected system to display the following message when the computer is booted:

W95/Babylonia by Vecna (c) 1999 Greetz to RoadKil and VirusBuster
Big thankz to sok4ever webmaster Abracos pra galera brazuca!!! --- Eu
Boto fogo na Babilonia!

Worm.Mypic or W32/Mypics.worm: The new virus, is set to disable computers as people try to start them up Jan. 1. The virus writer apparently is hoping to mislead users into thinking they've been hit by a Y2K software bug.

It arrives as a message without a subject line. The message body contains what appears to be an attachment called "Pics4You.exe" that is 34,304 bytes. If the executable file is opened, the worm loads into the computer's memory and attaches to the first 50 listings in address books of Microsoft Outlook users. After 20 minutes, the virus tries to e-mail itself again and repeats that after another 10 minutes, with that cycle continuing when "Mypic" is run.

Registry-key files must be deleted to get rid of MyPic after an infection. When Jan. 1, 2000 arrives, the virus will create a file called C:\CBIOS.COM, which will write over checksum data in BIOS setup information (CMOS), causing the error message "CMOS checksum is invalid" the next time the user tries to boot up the system. Checksum data is used to verify the integrity of computer data. That message is designed to make users think the problem is related to the year.

To reboot, the BIOS setup has to be invoked to fix the CMOS checksum. The next time a user successfully boots the machine, the worm will try to format both the C: and the D: drives.

DeadBoot.488: This is a multipartite virus. It infects the boot sectors of hard (Master Boot) and floppy disks (Boot) as well as executable files. In the case of this virus, the executable files it infects are those with EXE extensions. Once this is done, it goes memory resident and lays in wait to infect the boot sectors of all floppy disk accessed. Upon becoming resident in memory, the virus takes 1KB off the TOM (Top of Memory). It then goes on to hook the INT 13h interrupt (disk BIOS service), changing it for INT 9Ah.

W97M/Steriod.B: A macro virus that infects Microsoft Word documents. The virus infects the NORMAL.DOT word template and the results of the infection are, among others, the following: it removes the "Macro" and "Templates and Add-Ins" options that appear in the "Tools" menu in Word and it disables, but does not remove, "Options" from the "Tools" menu.

W97M/Steriod.B changes the name of the hard disk label or volume to the new name of "Testicle" and shows these messages:

"Can I have a bottle of warm Diet Mountain Dew?"
"Shout Out!... Slage Hammer, Spanska and the entire_Kim_Liberation _Army"

X97M/Laroux.DI: This is a macro virus that infects Microsoft Excel 97 books (spreadsheets). It is made up of a module called "PLDT" that includes the auto_open and check_files procedures. When an infected book is opened, X97M/Laroux.DI checks to see if a file called PLDT.XLS exists in the Microsoft Excel startup directory and if the book that is open contains modules. Depending on these data, two different scenarios may be produced, although in both cases the virus disables the screen refresh feature so that its actions are not noticeable. If the PLDS.XLS file does not exist and the current book does not contain modules, the virus infects the current book (the one that is open at the time) and saves it in the startup directory under the name of PLDT.XLS. Upon saving it, the virus gives it a standard read/write format, with no password or backup copy (BAK). On the contrary, if the PLDS.XLS file exists and the current book contains modules, the virus limits itself to infecting the current book.

MesMate Worm (a.k.a. NewApt): MesMate spreads, using the MS Outlook clients, as an attachment. The virus has already been found on the Internet and in some corporate environments, which means that there is real risk of infection.

If the user executes the attachment, unwittingly taking for granted that it is just an electronic joke or greeting e-card, an error message is displayed on screen.

After showing this message, MesMate modifies the Windows' registry so it activates each time the computer is started. Once the worm activates, it sends itself out to the e-mail addresses of the infected user's address book

Infected attachment is received enclosed in an e-mail message with one of the following bodies:
If you do not have an HTML capable e-mail client, the body displays the text

> "he, your lame client cant read HTML, haha. click attachment to see some stunningly HOT stuff"

If you have an HTML capable e-mail client, the body shows the text

> "http://www.stuart.messagemates.com/index.html Hypercool Happy Year 2000 funny programs and animations.... We attached our recent animation from this site in our mail ! Check it out!"

The attached infected file can have any of these names: baby.exe, bboy.exe, boss.exe, casper.exe, cheeseburst.exe, cooler1.exe, cooler3.exe, copier.exe, cupid2.exe, farter.exe, fborfw.exe, gadget.exe goal.exe, goal1.exe, g-zilla.exe, hog.exe, irnglant.exe, monica.exe, panther.exe, party.exe, pirate.exe, saddam.exe, theobbq.exe, video.exe. All they are the names of well-known jokes or greeting e-cards.

RAT.Drat: This a telnet-based Trojan that uses stealth code from Back Orifice 2000 to inject itself into the threads of live processes by changing the export locations in the operating systems global ATI table. Its execution is silent, during which time it copies itself to Windows\SHELL32.EXE, and modifies the two following registry entries: HKEY_CLASSES_ROOT exefile\shell\open\command\(Default)
HKEY_CLASSES_ROOT batfile\shell\open\command\(Default)
The value of these two keys normally defaults to "%1" %* Drat changes these values to SHELL32 "%1" %* What this means is that everytime a .exe or .bat file is executed, Windows executes the file through SHELL32.EXE, causing the Trojan to load each time.

Trojans

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #99-20 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Acid Battery	1.0	CyberNotes 99-25
Ambush		CyberNotes 99-25
Backdoor	0.1	CyberNotes 99-21
BioNet	0.84-0.92	CyberNotes 99-25
Bla	1.0-2.0	CyberNotes 99-22
BladeRunner		CyberNotes 99-22
Bobo		CyberNotes 99-20
Bobo	1.0-2.0	CyberNotes 99-25
BrainSpy	Beta	CyberNotes 99-21
Cain	1.50-1.51	CyberNotes 99-25
Deepthroat	3.1	CyberNotes 99-20
Der Spacher	3.0	CyberNotes 99-25
Doly	1.1-1.6	CyberNotes 99-20
Doly	1.1-1.7	CyberNotes 99-25
Donald Dick	**1.52-1.54**	**Current Issue**
Donald Dick	1.52	CyberNotes 99-20
Donald Dick	1.53	CyberNotes 99-22
Eclipse 2000		CyberNotes 99-20
GateCrasher	**1.0-1.1**	**Current Issue**
Girlfriend	1.3x (including patch 1)	CyberNotes 99-25
Hack'A'tack	**1.0-1.20**	**Current Issue**
HostControl	**1.0**	**Current Issue**
InCommand	1.0 (added 1.2)	CyberNotes 99-24
Ini Killer	2.0-3.0	CyberNotes 99-21
Irc3		CyberNotes 99-21
Logged		CyberNotes 99-21
Malicious		CyberNotes 99-25
Matrix	**1.4-1.7**	**Current Issue**
Matrix	1.4-1.5	CyberNotes 99-20
Matrix	1.4-1.7	CyberNotes 99-25
Millennium	1.0-2.0	CyberNotes 99-21
Naebi	2.12-2.34	CyberNotes 99-22
NetSphere	1.0-1.31337	CyberNotes 99-20
NetSpy	1.0-2.0	CyberNotes 99-22
Phaze Zero	1.0b - 1.1	CyberNotes 99-23
Revenger	1.0	CyberNotes 99-23
RingZero		CyberNotes 99-22
Ripper		CyberNotes 99-22
SpiritBeta	1.2f	CyberNotes 99-22
SubSeven	**1.0-2.1A**	**Current Issue**
SubSeven	1.0-2.0	CyberNotes 99-21
SubSeven	1.0-2.1	CyberNotes 99-25
Thing	1.00 - 1.60	CyberNotes 99-23
Transmission Scout	1.1 - 1.2	CyberNotes 99-23
Vampire	1.0 - 1.2	CyberNotes 99-23
WarTrojan	1.0-2.0	CyberNotes 99-21
Xanadu	**1.1**	**Current Issue**
Xplorer	1.20	CyberNotes 99-21
Xtcp	2.0-2.1	CyberNotes 99-24
Y2K Countdown (Polyglot)		CyberNotes 99-20
YAT		**Current Issue**

GateCrasher v1.0-1.1 (December 16, 1999): This appears to be an older Trojan, with most of the features NetBus boasts, and enough new features to fill the gaps. It can also keylog, grab passwords, and other monitoring tools for similar operations.

HostControl v1.0 (December 15, 1999): This is a simple basic Trojan with one new twist. The Trojan has a built-in windosk.ocx and related files, that if are missing on the infected systems, it will install its own. This way, there will be no errors loading on startup.

Xanadu v1.1 (December 15, 1999): This is another Trojan that acts pretty much like NetBus, just with an easier interface for the malicious user to control your computer.

YAT (December 15, 1999): YAT, which stands for Yet Another Trojan, though only boasting basic Trojan features, its main value is the fact it is extremely hard to remove. This Trojan is designed to copy itself to multiple places as backups and installs batch files to check for the Trojan, and reload it from a backup if not found.

Hack'a'Tack: Hack'a'Tack is a backdoor that allows attackers to move and kill windows on your desktop, open an FTP server on your machine, log keystrokes, save passwords you type, shut down the machine, and upload, download, and execute files. Hack'a'Tack only runs on Windows 95 and 98. It uses TCP port 31785 and UDP ports 31789 and 31791. If you connect to TCP port 31785, it will display a banner such as: hostxforce.org (In this example, xforce.org is the hostname of the machine). If you see TCP port 31785 and UDP ports 31789 and 31791 open when you run 'netstat -a', then you probably have Hack'a'Tack on your machine. (**Numerous scans for these particular ports have been reported recently, leading to the possibility that this Trojan is being widely used.)**

SubSeven v1.0-2.1A (December 15, 1999): The SubSeven Trojan has the exact feature list as NetBus, with one original feature. The server can send the malicious user your IP when you connect to the Internet by either/any of e-mail, IRC, or ICQ. New with version 2.1, the Trojan can be controlled not only via the SubSeven client, but also by messages sent to the IRC or ICQ drones the Trojan makes. This makes SubSeven very versatile and easy to use from a “malicious user'' standpoint.

Donald Dick v1.52-1.54 (December 6, 1999): A new remote administration tool, similar to BO2K or NetBus. The Trojan runs on Windows 95, 98 and NT 4.0 and allows full access to the File system, processes and threads, the registry, system information and a lot more.

Matrix v1.4-1.7 (December 6, 1999): This is a Trojan based on the sourcecode to the Girlfriend Trojan. Its main features seems to be an FTP like file server, and the ability to update the Trojan exe on a victim’s computer to a new version with one button click.